Please add the following new claims.

44. (New) The method of claim 1, further comprising the step of:
generating an authorization key;
providing the authorization key to the second party; and
encoding the authorization key with at least one of a plurality of criteria.

45. (New) The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion to indicate the information that can be accessed by the second party with the authorization key.

46. (New) The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion to indicate the number of times the authorization key can be used by the second party to obtain access.

47. (New) The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion designating the category of the first party's personal information that can be accessed by the second party using the authorization key.

REMARKS

Applicants have carefully reviewed the office action dated August 7, 2002. This response is believed to address all grounds for rejection stated in the office action and to place the application in a condition for allowance.

Statement in Office Action Regarding Admission of Prior Art

Applicants respectfully state that they did not admit that the Masters thesis of Naren Chaganti was "prior art." This statement is to clarify the record. The First Supplemental Information Disclosure Statement filed in May 19, 2000 stated, "Identification of listed references should not be construed as an admission that such references are available as 'prior art' against the instant application." Examiner is respectfully requested to reconsider this.

Sixth Supplemental Information Disclosure Statement

Applicants file concurrently herewith a Fifth Supplemental Information Disclosure Statement containing a (non prior art) reference that has come to Applicants' attention within the previous three months. Applicants respectfully request Examiner Darrow to review, examine and make the references of record in the instant application.

Telephone Interview on September 10, 2002

Applicants thank Examiner Darrow for courtesies shown during a telephone interview on September 10, 2002. Examiner Darrow has indicated in that discussion that a recitation—of different categories of information, without any correlation between the several categories of information, and that the different security levels could be applied [to the information objects] at any [level of] granularity in which information objects are secured—would clarify the instant claimed invention and would overcome the cited references.

Amendments to the Specification and Claims

In this response, Applicants:

a) Remove language informalities from the Specification;

b) Remove references to nonessential hyperlinks from the specification;

c) Indicate that products were trademarked as appropriate;

d) Clarify the independent claims as discussed during the telephone interview with the Examiner on September 10, 2002;

e) Amend claims 26-30 to comply with **In re Beauregard**;

f) Cancel Claim 25 without prejudice to overcome an obviousness-type double patenting rejection and add the same claim (with the above-mentioned clarification to the claim language) to a daughter application currently pending, i.e., Application Ser. No. 09/634,725, so that both these applications would be in a condition for allowance;

g) Cancel claims 12-13 without prejudice and added new claims 44-46 incorporating the language of the former claims 10, 12 and 13; and

h) Attach a clean copy of the currently pending claims.

No new matter is added as a result of these amendments.

Support for Additional Language in the Claims

In the September 10, 2002 interview, Examiner Darrow suggested certain clarification of a feature of invention. Applicants reserve their rights with regard to this clarification request. Applicants believe that the claims as they stand are patentably distinct over the cited prior art. Nevertheless, in an effort to bring at least some claims closer to issuance, Applicants have amended the claims to define the invention with added language. Applicants reserve the right to argue the claim language rejected in a continuation application and do not "concede[] an ability to claim the broader subject matter". *See Festo Corp. v. Shoketsu Kinzoku Kogyo Kaushiki Co.*, 122 S. Ct. 1831, 1840 (2002).

In the September 10, 2002 interview, Examiner appears to have suggested that the phrase:

> any granularity
>
> ***as applied to each information object to which at least one of a plurality of security levels is assigned*** would overcome the cited references and could render the instant claims allowable.

This additional language does not add new matter. Support for this language may be found in the Specification at page 8, lines 5-8.

Conclusion

Applicants have addressed all grounds for objection of the specification and rejection of claims 1-5, 7-11, 14-24, and 26-30. Three new claims 44-46 are added. These claims are currently pending in this application after the cancellation and recitation of claim 25 in a co-pending commonly owned continuation application. Two other claims, 12-13 are canceled to make them dependent on new claims 44-46 incorporating the language of claim 10.

In view of the aforementioned changes and remarks, Applicants believe that all currently pending claims in the instant are in a condition for allowance. Because the total number of claims remains the same, no further fee is due. Reconsideration and an early notice of allowance are respectfully solicited.

Respectfully Submitted,

(44,602)
Naren Chaganti
345 Sheridan Avenue, Suite 308
Palo Alto, CA 94306
(650) 248-7011 phone
(650) 838-0586 fax
naren@chaganti.com

Attorney for Applicants

Certificate of Mailing

I certify that this paper (together with any other papers mentioned or referenced herein as being enclosed) is faxed to the USPTO at (703) 746-7238.

November 6, 2002
Date

NAREN CHAGANTI

Clean Copy of the Currently Pending Claims

B1

1. A method for automatically disbursing a first party's personal information to a receiving party authorized by the first party by transmitting said first party's personal information from a server computer operated by a service provider, said server computer coupled to a database, the method comprising the steps of:

establishing an account for the first party with the server computer;

assigning an identifier to the first party;

entering the first party's personal information, said first party's personal information comprising at least one of a plurality of information objects;

assigning at least one of a plurality of security levels to each information object at any granularity, thereby enabling access to individually selected portions of the user's personal information by individual receiving parties;

storing in the database the first party identifier, the information object and the security level assigned to the information object;

receiving a request, said request comprising at least the first party identifier;

in response to the request, selecting a first portion of the first party's personal information objects that could be transmitted to a second party;

retrieving from the database the selected first portion of personal information objects; and

securely transmitting the retrieved first portion of personal information objects to the second party.

2. The method of claim 1, further comprising the steps of:
presenting an authorization by the second party; and
verifying the second party's authorization.

3. The method of claim 2, further comprising the steps of:

obtaining a second party identifier;

if the second party is not authorized to receive the information, recording the second party identifier; and

rejecting the second party's request for information.

12 con't

4. The method of claim 3, further comprising the steps of:

designating the second party as a junk requester if the second party presents a predetermined number of requests that are not authorized; and

generating an alarm indication.

7. The method of claim 1, further comprising the steps of:

generating an authorization key; and

providing the authorization key to the second party.

13 1 & con't

8. The method of claim 7, wherein the step of generating an authorization key comprises the steps of:

selecting at least one set of information objects, the set of selected information objects comprising at least one piece of the first party's personal information; and

creating a key to authorize access of the selected set of information objects.

9. The method of claim 7, wherein the step of generating an authorization key comprises the step of:

selecting the characteristics of second party that can present the authoization key for information.

10. The method of claim 7, further comprising the step of:

encoding the authorization key with at least one of a plurality of attributes.

3 Amn't

11. The method of claim 10, wherein the at least one of a plurality of attributes includes an attribute of a the second party who may present the authorization key to access the first party's information.

4

18. The method of claim 1, wherein the step of securely transmitting the information object further comprises the step of:

transmitting the information object via secure E-mail or public key encryption.

5 21 Amn't

23. The method of claim 1, wherein the step of receiving a request message from the second party comprises the step of:

receiving a query for the first party's personal information in a readily executable form.

6

26. A program storage device readable by a processor, said storage device tangibly embodying a program of instructions executable by the processor to perform the method steps for secure delivery of a first party's personal information via a communication network, said method steps comprising:

storing the first party's personal information, said first party's personal information comprising at least one of a plurality of information objects;

associating each information object with at least one of a plurality of security clearance levels at any granularity;

receiving a request message to access the first party's personal information, said request message comprising an authorization key to access a first portion of the first party's personal information, said authorization key indicative of a second security clearance level;

comparing the first security clearance level and the second security clearance level to determine an appropriate overall clearance level;

matching the request message and the overall clearance level with a second portion of the first party's personal information; and

securely transmitting the second portion of the first party's personal information.

27. The program storage device of claim 26, further comprising program of instructions executable by the processor to perform the method steps of:

authenticating the request message.

[illegible] ent

28. The program storage device of claim 26, further comprising program of instructions executable by the processor to perform the method step of:

establishing a secure audit trail of each access of the first party's personal information.

[illegible] ent

29. The program storage device of claim 28, wherein the program of instructions executable by the processor to perform the method step of establishing a secure audit trail include program of instructions executable by the processor to perform the method step of recording an identifier to identify a party that receives the first party's personal information.

30. The program storage device of claim 28, wherein the program of instructions executable by the processor to perform the method step of establishing the secure audit trail include program of instructions executable by the processor to perform the method step of recording an identifier to identify a second party.

44. The method of claim 1, further comprising the step of:

generating an authorization key;

providing the authorization key to the second party; and

encoding the authorization key with at least one of a plurality of criteria.

R1.126

D7
-am 4
&
cont

45. ~~48~~. The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion to indicate the information that can be accessed by the second party with the authorization key.

46. ~~49~~. The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion to indicate the number of times the authorization key can be used by the second party to obtain access.

47. ~~50~~. The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion designating the category of the first party's personal information that can be accessed by the second party using the authorization key.